

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-036000
 (43)Date of publication of application : 02.02.2000

(51)Int.Cl. 606F 19/00

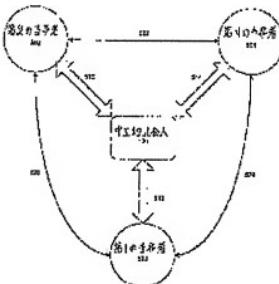
(21)Application number : 11-176128 (71)Applicant : SUN MICROSYST INC
 (22)Date of filing : 22.06.1999 (72)Inventor : LIPKIN EFREM

(30)Priority
 Priority number : 98 107692 Priority date : 30.06.1998 Priority country : US

(54) NEUTRAL OBSERVER IN ELECTRONIC COMMERCIAL TRANSACTION

(57)Abstract:

PROBLEM TO BE SOLVED: To obtain a method which allows a neutral observer to store the details of electronic commercial transaction by including a process which aims at fetching and provides recorded communication, etc., and making either of 1st and 2nd parties use a small client technology.
 SOLUTION: 1st and 2nd parties 500 and 502 are illustratively and respectively a client and a server. The N-th party 504 represents a server and probably the server is a server where a user maintains account with which electronic transaction is performed. A neutral observer 100 is connected to communication links 510, 512 and 514 so that the observer 100 can exist within communication paths that connect the parties. And, the transaction parties offer a transaction identifier to the neutral observer. Thus, the neutral observer can identify all of the parties of transaction, automatically extract related transaction details according to a specified protocol and store them.



(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2000-36000

(P2000-36000A)

(43)公開日 平成12年2月2日(2000.2.2)

(51)Int.Cl.
G 0 6 F 19/00

識別記号

F I
G 0 6 F 15/28
15/30マーク* (参考)
B
L

(21)出願番号 特願平11-176128
 (22)出願日 平成11年6月22日(1999.6.22)
 (31)優先権主張番号 09/107,692
 (32)優先日 平成10年6月30日(1998.6.30)
 (33)優先権主張国 米国(US)

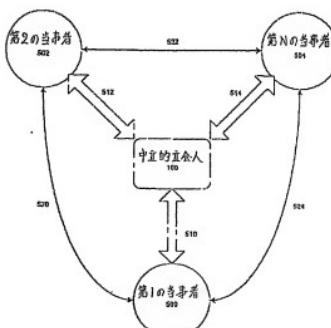
(71)出願人 595034134
 サン・マイクロシステムズ・インコーポレイテッド
 Sun Microsystems, Inc.
 アメリカ合衆国 カリフォルニア州
 94303 パロ アルト サン アントニオ
 ロード 901
 (72)発明者 エフレム リブキン
 アメリカ合衆国 カリフォルニア 94703,
 パークレー, ワード ストリート
 1811
 (74)代理人 100078282
 弁理士 山本 秀策

(54)【発明の名称】 電子商取引における中立的立会人

(57)【要約】

【課題】 電子商取引の詳細を中立的立会人により保存する方法を提供する。

【解決手段】 第1の当事者および第2の当事者を含む電子取引の詳細を保存する方法であって、第1の当事者と第3の当事者との間における第1の接続を確立する工程と、第2の当事者と第3の当事者との間における第2の接続を確立する工程と、第3の当事者における、第1の当事者および第2の当事者のうちの一方からの取引の詳細に関する通信を受け取る工程と、第1の当事者および第2の当事者の同意に基づく、第3の当事者を介しての通信を記録する工程と、取出を目的とした、記録された通信を提供する工程とを含み第1の当事者および第2の当事者のうちの一方が、小クライアント技術を用いる方法。



【特許請求の範囲】

【請求項1】 第1の当事者および第2の当事者を含む電子取引の詳細を保存する方法であって、

該第1の当事者と第3の当事者との間における第1の接続を確立する工程と、

該第2の当事者と該第3の当事者との間における第2の接続を確立する工程と、

該第3の当事者における、該第1の当事者および該第2の当事者のうちの一方からの該取引の詳細に関する通信を受け取る工程と、

該第1の当事者および該第2の当事者の同意に基づく、

該第3の当事者を介しての該通信を記録する工程と、取出を目的とした、該記録された通信を提供する工程と、

を含み、

該第1の当事者および該第2の当事者のうちの一方が、小クライアント技術を用いる、方法。

【請求項2】 前記取引に対する、信用性のある立会人としての前記第3の当事者を選択する工程を更に含む、請求項1に記載の方法。

【請求項3】 前記選択する工程が、前記取引の前ににおける、信用性のある立会人としての前記第3の当事者について合意する工程を含む、請求項2に記載の方法。

【請求項4】 前記第1の当事者および前記第3の当事者のうち一方が小クライアント技術を用いる、請求項1に記載の方法。

【請求項5】 前記通信の取り出す工程と、該通信を用いた前記詳細を提供する工程と、を更に含む、請求項1に記載の方法。

【請求項6】 前記詳細を提供する工程が、前記第3の当事者から、前記第1の当事者および前記第2の当事者のうちの一方へ前記通信を送信する工程を含む、請求項5に記載の方法。

【請求項7】 前記詳細を提供する工程が、前記第3の当事者における、前記第1の当事者または前記第2の当事者の一方からの、前記通信の申し立てられたコピーを受け取る工程と、

該申し立てられたコピーの正確さを検証する工程と、を含む、請求項5に記載の方法。

【請求項8】 前記第1の当事者を認証する工程を更に含む、請求項1に記載の方法。

【請求項9】 前記第1の当事者と前記第3の当事者との間における第1の接続を確立する工程が、該第1の当事者と該第3の当事者との間ににおける安全な通信リンクを確立する工程を含む、請求項1に記載の方法。

【請求項10】 前記通信リンクが、該通信リンクをわたら通信内における任意の変更の検出を容易にするプロトコルを介して、その安全を確保される、請求項9に記

載の方法。

【請求項11】 通信を受け取る工程が、前記取引の一部を証明する、通信のメッセージダイジェストを受け取る工程を含む、請求項1に記載の方法。

【請求項12】 前記メッセージダイジェストが、前記通信に対して行われるハッシュ機能の結果であるハッシュ値を含む、請求項1に記載の方法。

【請求項13】 前記メッセージダイジェストが、前記通信に対して行われる検査合計動作の結果である検査合

10 計を含む、請求項1に記載の方法。

【請求項14】 前記第3の当事者を介する、前記通信を記録する工程が、該通信を標準化する工程と、該通信をデータベースに記憶する工程と、を含む、請求項1に記載の方法。

【請求項15】 前記第3の当事者における、前記第1の当事者からの第1の取引識別子を受け取る工程と、前記第3の当事者における、前記第2の当事者からの第2の取引識別子を受け取る工程と、を更に含む、請求項1に記載の方法。

20 【請求項16】 前記第3の当事者における、前記第1の取引識別子と前記第2の取引識別子とを適合させる工程を更に含む、請求項15に記載の方法。

【請求項17】 電子取引に立ち会う方法であって、第1の取引当事者へ接続する工程と、第2の取引当事者へ接続する工程と、

該第1の当事者と該第2の当事者との間における通信を中継する工程と、

該第1の当事者と該第2の当事者との間でやり取りされた、該取引の1つ以上の条件を含むメッセージを受信す

30 る工程と、該1つ以上の条件を記録する工程と、を含む、方法。

【請求項18】 前記受信する工程が、前記第1の当事者と前記第2の当事者との間における、前記取引を行うためのプロトコルに一貫する通信を受け取る工程と、該通信に含まれる該取引の1つ以上の条件を、該プロトコルに従って識別する工程と、を含む、請求項17に記載の方法。

40 【請求項19】 前記記録する工程が、前記メッセージを指標化する工程と、

該メッセージをデータベースに記憶する工程と、を含む、請求項17に記載の方法。

【請求項20】 前記第1の当事者および前記第2の当事者のうちの一方が、小クライアント技術を用いる、請求項17に記載の方法。

【請求項21】 多数の当事者が関与する電子取引に立ち会う方法であって、第1の当事者からの該取引の、立ち会いの要求を受け取る工程と、

- 3 該第1の当事者を認証する工程と、
該第1の当事者からの第1の取引識別子の受け取る工程と、
第2の当事者からの接続を受け取る工程と、
該第2の当事者からの第2の取引識別子を受け取る工程と、
該取引の該当事者を識別するために、該第1の取引識別子と該第2の取引識別子を比較する工程と、
取引詳細を受け取る工程と、
該取引詳細を記録する工程と、
を含む、方法。
【請求項2 2】 前記取引詳細を受け取る工程が、前記第1の当事者と前記第2の当事者との間で交換された、前記取引の詳細を含む通信についてのメッセージダイジェストを受け取る工程を含む、請求項2 1に記載の方法。
- 【請求項2 3】 前記取引詳細を記録する工程が、前記メッセージダイジェストを指標化する工程と、
該メッセージダイジェストをデータベースへ記憶する工程と、
を含む、請求項2 2に記載の方法。
- 【請求項2 4】 前記メッセージダイジェストが前記通信の要旨である、請求項2 2に記載の方法。
- 【請求項2 5】 前記メッセージダイジェストが、前記通信に対して行われたハッシュ機能の結果であるハッシュ値を含む、請求項2 2に記載の方法。
- 【請求項2 6】 前記メッセージダイジェストが検査合計を含む、請求項2 2に記載の方法。
- 【請求項2 7】 取引詳細を受け取る工程が、前記第1の当事者または前記第2の当事者のうちの一方からの、前記取引の1つ以上の詳細または条件を含む通信を受け取る工程を含む、請求項2 1に記載の方法。
- 【請求項2 8】 前記取引詳細を記録する工程が、前記通信を指標化する工程と、
該通信をデータベースへ記憶する工程と、
を含む、請求項2 7に記載の方法。
- 【請求項2 9】 前記通信が、前記第1の当事者、前記第2の当事者、前記取引の時間、および該取引の日付からなる群のうちの1つ以上の要素によって指標化される、請求項2 8に記載の方法。
- 【請求項3 0】 前記第1の当事者および前記第2の当事者のうちの一方が小クライアント技術を用いる、請求項2 1に記載の方法。
- 【請求項3 1】 電子取引の詳細を記録するための方法を、コンピュータによって実行される場合に実施する命令を記憶する、コンピュータ読み取り可能記憶媒体であって、該方法が、
第1の当事者との第1の接続を確立する工程と、
第2の当事者との第2の接続を確立する工程と、
該第1の当事者および第2の当事者のうちの一方から
- 4 の、該取引の詳細に関する通信を受け取る工程と、
該通信を記録する工程と、
該第1の当事者および該第2の当事者のうちの一方による取出を目的とした、該記録された通信を提供する工程と、を含み該記録された通信が、該第1の当事者および該第2の当事者の同意に基づいて記録される、
コンピュータ読み取り可能記憶媒体。
【請求項3 2】 多数のエンティティを伴う取引を、後の検証のために保存する装置であって、
10 該多数のエンティティのそれぞれと通信するコンピュータシステムと、
該コンピュータシステム内における、該多数のエンティティのうちの1つを認証する、認証機構と、
該コンピュータシステム内における、該複数のエンティティのうちの該1つから該取引に関する通信を受け取る、受取機構と、
該コンピュータシステム内における、該通信を記憶する、記憶機構と、
該コンピュータシステム内における、該通信を取り出す、取出機構と、
を含む、装置。
【請求項3 3】 電子取引に立ち会うためのコンピュータシステムであって、
プロセッサと、
該コンピュータシステムと第1の取引当事者とを接続する、第1の信用通信リンクと、
該コンピュータシステムと第2の取引当事者とを接続する、第2の信用通信リンクと、
該第1の取引当事者または該第2の取引当事者のうちの一方から受け取られる、該取引の詳細に関する通信を記録する、記憶デバイスであって、該通信が、該詳細を検証するために取り出される場合のために記憶される、記憶デバイスとを含む、
コンピュータシステム。
【請求項3 4】 前記第1の信用通信リンクまたは前記第2の信用通信リンクのうちの一方で受け取られた通信を、該第1の信用通信リンクまたは該第2の信用通信リンクのうちの他方に中継する、中継装置、
を含み、
40 該コンピュータシステムが、前記第1の取引当事者と前記第2の取引当事者との間で交換された全通信を受け取る、
請求項3 3に記載の、コンピュータシステム。
【請求項3 5】 前記記憶デバイスがデータベースを含む、請求項3 3に記載のコンピュータシステム。
【請求項3 6】 前記第1の取引当事者および前記第2の取引当事者のうちの一方が小クライアント技術を用いる、
請求項3 3に記載のコンピュータシステム。
【請求項3 7】 多数の当事者を伴う電子取引の1つ以上

該多数の当事者の1人の身元を検証するための、検証手段と、

該多数の当事者のそれそれから、該1つ以上の取引詳細に関する信用通信を受け取るための、受取手段と、

該信用通信を記録する、記録手段と、

該記録された1つ以上の詳細を取り出す、取出手段と、を含む装置であって、

該装置が、該信用通信を受け取り、該取引の該1つ以上の詳細を後に検証する目的で該信用通信を記録するためには、該多数の当事者のそれそれと接続される、装置。

【請求項38】前記多数の当事者の1人が小クライアント技術を含む、請求項37に記載の装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はコンピュータシステムおよび電子商取引の分野に関する。より具体的には、電子取引への当事者が取引の条件を拒否することを防ぐシステムおよび方法が提供される。

【0002】

【從来の技術】コンピュータ間の相互接続の拡大は、ビジネスおよび他の業務上の取引のための新たな電子経路を提供してきた。しかし、電子取引は、互いに面識の無い、且つしたがって、互いを信用する基盤を全く有さない2つの当事者の間でしばしば行われている。したがって、電子取引は安全面での問題点、および法的な問題点を伴い、それらの問題点は、人対人、電話による手段、または人間の仲介者など、より伝統的な方法を介して行われる取引において遭遇する問題点とは幾分異なったものである。

【0003】

【発明が解決しようとする課題】多くの取引または契約に共通する問題点の1つは、それが電子取引であるかそれ以外での取引であるかにかかわらず、取引の条件を提供することにある。取引への当事者は同一の条件に対し同意したと信じ得るが、同意された条件に関する係争が、依然、不定期の頻度で生じている。典型的に、そのような係争は、一方の当事者が契約のうちの自らの部分を、または自らの部分であると信じている部分を実行するまで、起らない。

【0004】契約の1つの条件または複数の条件に関して、当事者の間で係争が起きる場合、当事者のそれぞれは、一般的に、自らの理解および信じるところが契約の真の性質を反映することを證明しようと試みる。紙面を基にする取引の世界では、通常、一方の当事者、または当事者の双方が、契約に関する何らかの書類を有する。頗るくば、そのような書類が係争の焦点である条件の真の性質を反映し、且つ当事者双方の応諾（例えば、署名など）を証明する。法的な係争は書類が存在する場合でさえも依然生じ得るが、書類が無い場合には法的係争はほぼ必ずである（契約に伴う価値が些細なものでないとい

仮定して）。

【0005】しかし、電子取引の世界では、契約は電気信号および送信を介して行われる。1人の当事者は、他の当事者を誤って通信に接続する方法なしに電子取引に関する通信を記録し得るが（紙面、または別の手段に）、他の当事者は、その参加を拒絶し得るか、または取引の中心的部分を拒否し得る。したがって、1人の当事者による、取引に関する電子通信の記録それ自体は、その通信において反映された条件に他の当事者を拘束するためには一般に不十分である。信用性のある当事者が通信または取引の内容を証言し、その内容を證明（または、少なくとも強力な證拠を提供する）することなくして、当事者の間の係争は容易に解決しない。

【0006】例えば、インターネット上にはデジタル情報を記録する目的でアーカイブサービスが存在するが、それはその拒絶を妨げるために取引を提供し、再生する方法をほとんど提供しない。例えば、Uniform Resource Locator(URL)として公知のアーカイブサービス、<http://www.archive.org/>は、インターネットの歴史または進化を収集または文書化する目的で、インターネットからデジタルデータの様々な部分（例えば、ウェブページ）を記録する。このサービスは、信用性のある方法であるかどうかにかかわらず、取引への参加者に代わって特定の電子取引の詳細を記録することは全くせず、したがって、参加者が約束を破ることを防止するためにその電子取引を再生することはできない。

【0007】別の例として、電子オークションシステムでは、プローカーが1人以上の当事者と1つのアイテムの販売について交渉する（すなわち、入札を受け付ける）。プローカーは販売者に代わって取引を行い、販売者および購入者は交渉または別の直接的なやり取りは行わない。したがって、オークションの取引は2人の当事者（購入者およびプローカー）の間で行われ、そこで、プローカーは、信用性のあるまたは利害関係のない第三者としてよりも、販売者の代理人として行動する。取引の詳細または条件は保管され得るかまたは保管され得ず、且つ取引の再生を許可し得るかまたは許可し得ない、詳細が記録されている場合、それは2人の当事者のうち1方によって記録される。プローカーは基本的に販売者の代理人として行動するので、購入者には、取引に関するプローカーの記憶または記録を信頼する理由はない。

【0008】米国特許第5,629,980号は、デジタル作業の分配およびその使用を制御するシステムを示す。このシステムはデジタル作業の収容場所を伴い、1つの収容場所におけるデジタル作業は別の収容場所によってアクセスされ得る（例えば、コピー、または貸すことによって）。システムの1つの実施態様では、そのような取引が完了した場合、両方の収容場所は請求情報をクリエットサーバに送り、それにより請求処理の回避を

40
40
40
40
50

防ぐ。したがって、このシステムでは請求情報のみが第三者に提供され、その目的は、取引の詳細を再生することではなく、正確な請求を確実にすることである。取引の他の詳細は、それが少しでも保存されている場合、1つの収容場所または他の収容場所によって記録されなければならない。加えて、取引の任意の詳細を再生することはできない。

【0009】DigiCash, Inc.によって提供されるようなデジタルキャッシュシステムも、また、当事者間の係争における、取引の再生は行い得ない。加えて、デジタル銀行は取引に立ち会い、または監視するようには意図されていない。デジタル銀行は消費者にデジタルキャッシュを提供した旨の記録および／または小売商からデジタルキャッシュを受け取った旨の記録を維持する。しかし、一般的に、銀行は特定の取引への当事者を識別し得ない。従来の通貨と同様に、銀行は消費者に以前提供した通貨を小売商から受け取り得るが、銀行は、所有する情報をから、特定の取引に参加している消費者および小売商を識別し得ない。

【0010】電子取引上の係争を防ぐ目的で、取引に関する全通信を単純に記憶することとも、また、電子取引の世界に間与する多くの人間にとて速いた解決方法とは言えない。特に、「小クライアント(thin client)」技術を用いているユーザおよびアプリケーションは、典型的には、そのような通信を記憶するためのリソース(例えば、記憶能力)および／またはソフトウェアを有さない。

【0011】例えば、Secure Electronic Transactions(SET)環境において、消費者と小売商との間の取引に関するオーダー情報(OI)は、支払い取得手段(例えば、クレジットカードサービス)に提供される。消費者がこの情報を提供するために、細密な算出能力が必要とされる。例示的に、取引の詳細を含む「オーダー説明(HOD)」はハッシュされたオーダー説明(HOD)に変換され、それは、支払い取得手段にに対して提供されるOIに含まれる。また、一般的に、徹底した暗号による保安がSETでは必要とされ、更に、消費者対してその要求が増加している。したがって、小クライアントは、必要な算出リソースが欠如しているので、このような形態のSETに参加することはできない。加えて、支払い取得手段は、取引の詳細を正確に記録および／または再生するとして消費者から信用されるという点で、「信用性のある」当事者ではない。

【0012】本発明は上記の課題に鑑みてなされたものであり、その目的は上記のような問題点を克服して、電子商取引の詳細が中立的立会人により保存される方法を提供することである。

【0013】

【課題を解決するための手段】第1の当事者および第2の当事者を含む電子取引の詳細を保存する方法であつ

て、該第1の当事者と第3の当事者との間における第1の接続を確立する工程と、該第2の当事者と該第3の当事者との間における第2の接続を確立する工程と、該第3の当事者における、該第1の当事者および該第2の当事者のうちの一方からの該取引の詳細に関する通信を受け取る工程と、該第1の当事者および該第2の当事者の同意に基づく、該第3の当事者を介しての該通信を記録する工程と、取出を目的とした、該記録された通信を提供する工程と、を含み、該第1の当事者および該第2の当事者のうちの一方が、小クライアント技術を用い、それにより上記目的が達成される。

【0014】前記取引に対する、信用性のある立会人としての前記第3の当事者を選択する工程を更に含んでもよい。

【0015】前記選択する工程が、前記取引の前における、信用性のある立会人としての前記第3の当事者について合意する工程を含んでもよい。

【0016】前記第1の当事者および前記第3の当事者のうち一方が小クライアント技術を用いてもよい。

【0017】前記通信の取り出す工程と、該通信を用いた前記詳細を提供する工程と、を更に含んでもよい。

【0018】前記詳細を提供する工程が、前記第3の当事者から、前記第1の当事者および前記第2の当事者のうちの一方へ前記通信を送信する工程を含んでもよい。

【0019】前記詳細を提供する工程が、前記第3の当事者における、前記第1の当事者または前記第2の当事者の一方からの、前記通信の申し立てられたコピーを受け取る工程と、該申し立てられたコピーの正確さを検証する工程と、を含んでもよい。

【0020】前記第1の当事者を認証する工程を更に含んでもよい。

【0021】前記第1の当事者と前記第3の当事者との間における第1の接続を確立する工程が、該第1の当事者と該第3の当事者との間における安全な通信リンクを確立する工程を含んでもよい。

【0022】前記通信リンクが、該通信リンクをわたる通信内における任意の変更の検出を容易にするプロトコルを介して、その安全を確保されてもよい。

【0023】通信を受け取る工程が、前記取引の一部を証明する、通信のメッセージダイジェストを受け取る工程を含んでもよい。

【0024】前記メッセージダイジェストが、前記通信に対して行われるハッシュ機能の結果であるハッシュ値を含んでもよい。

【0025】前記メッセージダイジェストが、前記通信に対して行われる検査合計動作の結果である検査合計を含んでもよい。

【0026】前記第3の当事者を介する、前記通信を記録する工程が、該通信を指標化する工程と、該通信をデータベースに記憶する工程とを含んでもよい。

【0027】前記第3の当事者における、前記第1の当事者からの第1の取引識別子を受け取る工程と、前記第3の当事者における、前記第2の当事者からの第2の取引識別子を受け取る工程とを更に含んでもよい。

【0028】前記第3の当事者における、前記第1の取引識別子と前記第2の取引識別子とを適合させる工程を更に含んでもよい。

【0029】電子取引に立ち会う方法であって、第1の取引当事者へ接続する工程と、第2の取引当事者へ接続する工程と、該第1の当事者と該第2の当事者との間ににおける通信を中継する工程と、該第1の当事者と該第2の当事者との間でやり取りされた、該取引の1つ以上の条件を含むメッセージを受諾する工程と、該1つ以上の条件を記録する工程とを含んでもよい。

【0030】前記受諾する工程が、前記第1の当事者と前記第2の当事者との間ににおける、前記取引を行うためのプロトコルに一貫する通信を受け取る工程と、該通信に含まれる該取引の1つ以上の条件を、該プロトコルに従て識別する工程とを含んでもよい。

【0031】前記記録する工程が、前記メッセージを指標化する工程と、該メッセージをデータベースに記憶する工程とを含んでもよい。

【0032】前記第1の当事者および前記第2の当事者のうちの一方が、小クライアント技術を用いてもよい。

【0033】多数の当事者が関与する電子取引に立ち会う方法であって、第1の当事者からの該取引の、立ち会いの要求を受ける工程と、該第1の当事者による認証する工程と、該第1の当事者からの第1の取引識別子の受け取る工程と、第2の当事者からの接続を受け取る工程と、該第2の当事者からの第2の取引識別子を受け取る工程と、該取引の該当事者を識別するために、該第1の取引識別子と該第2の取引識別子を比較する工程と、取引詳細を受け取る工程と、該取引詳細を記録する工程とを含んでもよい。

【0034】前記取引詳細を受け取る工程が、前記第1の当事者と前記第2の当事者の間で交換された、前記取引の詳細を含む通信についてのメッセージダイジェストを受け取る工程とを含んでもよい。

【0035】前記取引詳細を記録する工程が、前記メッセージダイジェストを指標化する工程と、該メッセージダイジェストをデータベースへ記憶する工程とを含んでもよい。

【0036】前記メッセージダイジェストが前記通信の要旨であってもよい。

【0037】前記メッセージダイジェストが、前記通信に対して行われたハッシュ機能の結果であるハッシュ値を含んでもよい。

【0038】前記メッセージダイジェストが検査合計を含んでもよい。

【0039】取引詳細を受け取る工程が、前記第1の当

事者または前記第2の当事者のうちの一方からの、前記取引の1つ以上の詳細または条件を含む通信を受け取る工程を含んでもよい。

【0040】前記取引詳細を記録する工程が、前記通信を指標化する工程と、該通信をデータベースへ記憶する工程とを含んでもよい。

【0041】前記通信が、前記第1の当事者、前記第2の当事者、前記取引の時間、および該取引の日付から成る群のうちの1つ以上の要素によって指標化されてもよい。

【0042】前記第1の当事者および前記第2の当事者のうちの一方が小クライアント技術を用いてもよい。

【0043】電子取引の詳細を記録するための方法を、コンピュータによって実行される場合に実施する命令を記憶する、コンピュータ読み取り可能記憶媒体であって、該方法が、第1の当事者との第1の接続を確立する工程と、第2の当事者との第2の接続を確立する工程と、該第1の当事者および第2の当事者のうちの一方からの、該取引の詳細に関する通信を受け取る工程と、該通信を記録する工程と、該第1の当事者および該第2の当事者のうちの一方による取出目的とした、該記録された通信を提供する工程と、を含み該記録された通信が、該第1の当事者および該第2の当事者の同意に基づいて記録され、それにより上記目的が達成される。

【0044】多數のエンティティを伴う取引を、後の検証のために保存する装置であって、該多數のエンティティのそれぞれと通信するコンピュータシステムと、該コンピュータシステム内における、該多數のエンティティのうちの1つを認証する、認証機構と、該コンピュータシステム内における、該複数のエンティティのうちの該1つから該取引に関する通信を受け取る、受取機構と、該コンピュータシステム内における、該通信を記憶する、記憶機構と、該コンピュータシステム内における、該通信を取り出す、取出機構とを含み、それにより上記目的が達成される。

【0045】電子取引に立ち会うためのコンピュータシステムであって、プロセッサと、該コンピュータシステムと第1の取引当事者とを接続する、第1の信用通信リンクと、該コンピュータシステムと第2の取引当事者とを接続する、第2の信用通信リンクと、該第1の取引当事者または該第2の取引当事者のうちの一方から受け取られる、該取引の詳細に関する通信を記録する、記憶デバイスであって、該通信が、該詳細を検証するために後に取り出される場合のために記憶される、記憶デバイスとを含み、それにより上記目的が達成される。

【0046】前記第1の信用通信リンクまたは前記第2の信用通信リンクのうちの一方で受け取られた通信を、該第1の信用通信リンクまたは該第2の信用通信リンクのうちの他方に中継する中継装置を含み、該コンピュータシステムが、前記第1の取引当事者と前記第2の取引

11

当事者との間で交換された全通信を受け取ってもよい。
【0047】前記記憶デバイスがデータベースを含んでよい。

【0048】前記第1の取引当事者および前記第2の取引当事者のうちの一方が小クライアント技術を用いてもよい。

【0049】多数の当事者を伴う電子取引の1つ以上の詳細を保存する装置であって、該多数の当事者の1人の身元を検証するための、検証手段と、該多数の当事者のそれそれから、該1つ以上の取引詳細に関する信用通信を受け取るための、受取手段と、該信用通信を記録する記録手段と、該記録された1つ以上の詳細を取り出す取出手段とを含む装置であって、該装置が、該信用通信を受け取り、該取引の該1つ以上の詳細を後に検証する目的で該信用通信を記録するために、該多数の当事者のそれそれに対接され、それにより上記目的が達成される。
【0050】前記多数の当事者の1人が小クライアント技術を含んでよい。

【0051】本発明によると、電子取引における拒絶を防ぐシステムおよび方法が提供される。特に、1人の当事者または全当事者が、取引の今までの経緯に関するデータを維持することを要求しない電子取引における、拒絶を防ぐ方法が提供される。加えて、発明の特定の実施態様における、電子取引の拒絶を防ぐ方法およびシステムは、その取引に参与する当事者による膨大なリソースまたは処理能力を必要としない。

【0052】発明の1つの実施態様において、「中立的立会人」は、電子取引（例えば、インターネットまたは他の地域ネットワークを介して行われる）への信頼性のある立会人として提供される。この実施態様にしたがって、中立的立会人は、取引に参与する2人以上の当事者と信用リンクを確立する。例示的には、当事者を認証し、且つ当事者への信用リンクを形成するために、Secure Sockets Layer (SSL) プロトコルが用いられる。

【0053】発明の本実施態様では、中立的立会人（例えば、インターネットサービス）が立会人として機能し始める場合、第1の当事者（例えば、インターネットに接続する小売商）は中立的立会人に取引識別子を受け渡す。この取引識別子は取引および取引に参与する当事者を識別するために用いられる。同一の取引の他の当事者（例えば、クライアントを介して、インターネットに接続されるユーザ）が中立的立会人に接続する（例示的に、また、信用リンクを用いる）にしたがい、これらの当事者は同一の取引識別子を提供する。したがって、中立的立会人は全取引当事者を識別し得る。

【0054】一旦、全当事者が中立的立会人に接続されると、取引の1つ以上の詳細が、1人以上の当事者によって、中立的立会人に受け渡される。その詳細は、中立的立会人によって指標化され、記録される。

【0055】1つの実施態様では、中立的立会人は全通

50

12

信（例えば、ウェブページ、http要求）を受け取り、記録する。別の実施態様では、当事者は、中立的立会人に對して、取引の1つ以上の詳細を含む、通信のダイジェストを受け渡す。例示的に、ダイジェストはメッセージダイジェストであり、そのメッセージダイジェストは取引の「指紋を採取」するように機能する。または、ダイジェストは通信の要旨または抜粋である。

【0056】取引を行うために特定のプロトコルが用いられる場合、中立的立会人または一方の当事者は、プロトコルにしたがって、関係のある取引詳細を自動的に取り出しある。

【0057】

【発明の実施の形態】以下の説明は、当業者が本発明を実施し、用いることを可能にするために提供され、特定の適用例および必要条件の観点から提供される。開示される実施態様に対する様々な変容が当業者には容易に明らかとなり、且つ、本明細書中に規定される包括的な原理は、本発明の精神および範囲から逸脱することなく、他の実施態様および用途に適用可能である。したがって、本発明は示される実施態様に限定されるものではなく、本明細書中に開示される原理および特徴に一致する最大の範囲に適合するように意図される。

【0058】例えば、本発明の1つの実施態様は、インターネット上で行われる電子取引の拒絶を防ぐための「中立的立会人」の観点で説明される。その電子取引は、一方の当事者が、他方の当事者から物品またはサービスを購入するような取引などである。しかし、発明の範囲は、特定の種類の電子取引、または電子取引を行なう方法に限定されない。更に、本実施態様を説明する際に、様々な通信リンクが示される。本発明の実施態様は、インターネット通信の観点から、およびインターネットにアクセスする方法の観点から説明されるが、本発明の範囲は、特定の種類のネットワークまたは通信リンクに限定されない。

【0059】この詳細な説明にわたって、本発明の完全な理解を提供するために、特定の保護プロトコルまたは認証技術など、數々の特定の詳細が提示される。しかし、当業者には、本発明はそのような特定の詳細なしに実施され得ることが理解される。他の例では、本発明が不明瞭になることを防ぐために、周知の制御構造およびシステム構成要素は詳細に示されない。

【0060】また、本発明の技術は、様々な技術を用いることにより実行され得ることを理解されたい。例えば、本明細書中に更に説明される中立的立会人は、コンピュータシステム上で実行されるソフトウェアにおいて実行され得るか、または、マイクロプロセッサ、あるいは他の特別に設計されたアプリケーションの限定的な集積回路の組み合わせ、プログラム可能ロジックデバイス、またはそれらの様々な組み合わせのいずれかを用いるハードウェアにおいて実行され得る。特に、本明細書中に

説明される中立的立会人は、キャリアウエーブまたはディスクドライなどの記憶媒体上における一連のコンピュータ実行可能命令によって、実行され得る。

[0061] 中立的立会人の脱明

発明の1つの実施態様では、電子取引に立ち会い、その取引に関与する当事者が取引またはその必須の部分を拒絶することを防ぐために、「中立的立会人」が提供される。典型的な電子取引または契約では、互いの間の合意に関する条件を交渉し、且つ実行するために、2人以上の当事者が電子通信を交換する。この合意に引き続き、当事者は、それぞれの役割を実行する。例えば、インターネットを介して行われる品物またはサービスの販売において、販売者が特定の値段においてその品物またはサービスを提供するか、購入者が特定の値段におけるその品物またはサービスの購入を提供する。次いで、他方の当事者が応答し、可能性として、その提供を受け入れるか、またはそれに対応する提供を提示する。当事者が、関連する条件（例えば、値段、質、説明、配送手段、支払い方法）について合意したあと、販売者はその品物を配送するか、またはサービスを提供し、購入者は支払いを行う。

[0062] 本発明は、電子取引の当事者が、契約が実行された後に、その契約または契約の重要な部分を拒絶することを防ぐためのシステムおよび方法を提供する。中立的立会人は取引の当事者ではなく、当事者の合意の条件を含む、1つの通信または複数の通信の全部分または1部を記録、要約、または保存する。中立的立会人は、取引の全当事者から信用されるエンティティ（例えば、銀行または対面取扱手段）によって動作されることが好ましく、それにより取引の詳細を記憶、取り出し、および／または再生する安全な環境を提供する。

[0063] 図1は、本発明の1つの実施態様を示す。本実施態様では、中立的立会人100は、電子取引に関与するクライアントとサーバとの間でやり取りされる通信の経路内に位置づけられる。図1に示される取引は、例示的に、クライアント120およびサーバ140を含み、それぞれ、通信リンク110および130によって中立的立会人100に接続される。示される実施態様は2人の当事者のみを含むが、別の実施態様では、2人以上の当事者が関与する。

[0064] 例示的に、中立的立会人100は、プロセッサ102、認証手段104、およびデータベース106を含む。加えて、中立的立会人100は、当事者との通信用に多数の通信ポート（図1には示さず）を含む。プロセッサ102は、中立的立会人100を動作させる一連のコンピュータ読み取り可能命令を実行する。認証手段104は接続されている当事者の身元を検証するよう働く。例示的に、認証手段104は、中立的立会人100を用いている当事者によって提供される証明書のデジタル署名を認証することによって、当事者を証明す

る。

[0065] データベース106は、中立的立会人100によって立ち会われた取引の詳細を記憶するデータ記憶領域を含み、且つそのような詳細を指標化する手段を含む。本発明の1つの実施態様において、取引の詳細は、暗号化されたフォーマットでデータベース106内に記憶される。例示的に、取引の詳細は、Digital Encryption Standard (DES)で提供されるような対称キーによって暗号化される。または、Public Key Encryption (PKE)法がどのように用いられようと、その取引の詳細のコピーが取引の全当事者に付与される。PKEでは、取引の詳細が中立的立会人100の私的なキーによって例示的に暗号化され、対応する公的なキーによってのみ解読され得る。

[0066] 例示的には、クライアント120は、サーバ140にアクセスするためのウェブブラウザまたは他のインターネットを介すを含む。サーバ140はインターネットサーバ（例えば、ウェブサーバ）であり、中立的立会人100はインターネットサーバまたはアプリケーションである。したがって、示される実施態様では、通信リンク130はインターネットであり、通信リンク110はインターネット接続（例えば、インターネットサービスプロバイダを介する専用リンクまたはダイヤルアップリンク）である。中立的立会人100、クライアント120、およびサーバ140は、本発明の実施態様では、はっきりと区別されるエンティティであるが、別の実施態様では、それらのうち、任意のもの、または全部が区別を持たないものである（例えば、1つのコンピュータシステムおよび／またはネットワークにおいて、共同で位置づけられる）。例えば、本発明の1つの実施態様では、中立的立会人100はネットワークサーバを構成する。ユーザは、同じネットワークサーバ上で電子商取引に参加するためのアカウントを維持し、且つサーバ140と同じコンピュータ上で動作する。本発明の範囲は、中立的立会人100、クライアント120、およびサーバ140を相互接続するための、特定の種類または形態の通信リンクに限定されるものではない。

[0067] 上述のように、ここで説明される実施態様では、中立的立会人100は、クライアント120とサーバ140との間で行われる全通信を受け取り、且つ転送する。したがって、中立的立会人100は、電子取引の条件の全部分または1部を反映する通信を傍受し、且つ保存し得る。例示的には、中立的立会人100は合意の中心的条件を維持する（例えば、値段、質、説明、配達または実行の時間枠）。例えば、Open Trading Protocol (OTP)またはElectronic Data Interchange(EDI)の1つの形態などの特定のプロトコルが取引に対して実行される場合、中立的立会人100は、取引の少なくとも中心的条件を識別し、且つ維持するため、そのプロトコルを適用するよう構成される。条件は1つの通信また

は多数の通信に反映され得る。特に、中立的立会人100によって維持される通信は、条件に対する当事者の合意を正確に反映する。例えば、例示的に、中立的立会人100はクライアント120によって提出されたオーダーフォーム（例えば、ユーザによって作成されたエントリを備える、購入を示すウェブページ）、およびサーバ140からの検証を記憶する。または、中立的立会人100は当事者間の取引の開始時から終了時までわたる全通信を記録する。

【0068】中立的立会人100は当事者の取引における中心的条件を維持するので、ユーザと小売商との間で係争が生じた際には、取引を「再生成」し得る。例えば、ユーザは、合意したよりも高い値段で請求され得、または彼らが予期していた物品とは異なる物品を受け取り得る。そのような場合、ユーザは中立的立会人100に、合意事項を、またはそのうちの関連部分を再生するよう要求する。信用度および安全性を含む、中立的立会人100の信用性により（更に後述する）、再生成された取引が不正確であることを証明する責任は、中立的立会人の記録に同意しない当事者に課せられる。

【0069】当事者は、本発明によって提供されるような中立的立会人の使用が、クライアント120が「小」クライアントである場合に特に有効であることを認識する。「大」クライアントはより強力なリソースを有し、且つ、それにより電子取引の条件を含む通信を維持し得る傾向にあるが、小クライアントは一般的にそのような能力に欠ける。したがって、発明の本実施態様における中立的立会人の実行は、クライアント120に対して、追加のソフトウェアまたはプログラミングを要求しない。或いは、保存しておくことをユーザが望む通信があることを中立的立会人100に通達するために、アプレットがクライアント120によって用いられる。

【0070】本発明の別の実施態様が図2に示される。この実施態様において、中立的立会人100は、取引の当事者（クライアント120およびサーバ140）の間での全通信の経路内には位置づけられない。その代わりに、クライアント120とサーバ140との間で取り交わされた通信は、通信リンク200で通信される。したがって、当事者は、中立的立会人100からは独立して取引の条件についての合意に達する。通信リンク200は、例示的に、ダイヤルアップリンク、または他のリンクの組み合わせを含む。1つの実施態様では、通信リンク200は、クライアント120とインターネットサービスプロバイダ（ISP）との間の接続、およびISPとサーバ140との間の連絡を含む。

【0071】図2に示される実施態様では、クライアント120およびサーバ140は、彼らの取引の詳細を、中立的立会人100に対して独立に送信する。したがって、取引を含む元来の通信を受け取りはしないものの、中立的立会人は、依然、後に取引の全部分または一部を

証明するために必要となる情報を受け取る。本発明の本実施態様は、また、小クライアントに良好に適していることが理解される。例示的に、ここで説明される実施態様におけるクライアント120は、アプレットを用いるブラウザである。アプレットは、所望の取引詳細を中立的立会人100に転送する。

【0072】図2では、中立的立会人100に、当事者双方が取引の詳細を提出するように示すが、本発明の別の実施態様では、クライアント120など、1人の当事者のみが取引の詳細を提出する。そのような実施態様において、サーバ140は取引に関する自らの記録を維持し得る。しかし、この実施態様では、中立的立会人100の信用性から、取引の詳細に関する立会人の報告がサーバの報告と異なる場合、立会人の報告の方が好まれる（例えば、法的係争の際、裁判所で）。

【0073】情報を取り扱う実際の参加者から受け取ることを確実にするために、中立的立会人100は、例示的に、サーバ140が通信リンク130を介して接続を確立する場合にサーバ140を認証し、クライアント120が通信リンク110を介して接続する場合にクライアント120を認証する。本実施態様ではSecureSockets Layer (SSL)認証が用いられるが、他の方法（例えば、デジタル証明書、固定インターネットプロトコル(IP)アドレス）も同様に考慮される。

【0074】取引の条件がクライアント120およびサーバ140の双方によって提出される場合、本発明の1つの実施態様では、中立的立会人100は当事者によって提出された報告を比較する。双方の報告が同一の詳細を反映している場合、その後中立的立会人100は例示的に一方の報告のみを記憶する。しかし、詳細が異なる場合、中立的立会人100は、例示的に、後の調停のために双方の報告を記憶するように構成される。それは、必要となり得るか、またはなり得ない場合もある。または、中立的立会人100は、不合意を未然に防止するために、当事者にその差異を報告する。

【0075】クライアント120とサーバ140との間でやり取りされる全情報が記録されない限り、中立的立会人に送付され、記録されるような通信（例えば、ウェブページ）または取引詳細を識別する方法が必要とされる。上述のように、取引プロトコルは当事者によって実行され得、その場合、クライアント120およびサーバ140は、記録されるべき重要な情報の識別のためにそのプロトコルを適用する。プロトコルが実行できない別の実施態様では、ユーザが記録したいと思うウェブページのそれぞれは、ある様式でマークが付される（例えば、取引の各ページに、チェックボックスがプログラムされる）。他の、別の実施態様では、例示的に、小売商はクライアントから受け取った全通信を中立的立会人に転送する。

【0076】異なる別の実施態様では、サーバ140は

クライアント120に対して、中立的立会人100によって記録されるべき情報に関する1つ以上のオプションを提供する。オプションは、中立的立会人によって中繼され得る。クライアントが選択を退信した後、対応する情報が自動的に中立的立会人に送付される。

【0077】中立的立会人の動作

図3は、図2に示される本発明の実施態様にしたがって中立的立会人を実行し、それによって電子取引の中心的部分の保存を可能にする、例示的な方法を示す。その方法をより詳細に表すフローチャートは図4に提供され、且つ以下に更に説明される。例示的に、方法は、インターネットおよびインターネットベースの商取引の觀点から適用される。

【0078】初期の段階で、ユーザは、サーバ140上のウェーブページまたは他の情報をブラウズするために、クライアント120を用いる。ユーザによるブラウズ行為は通信リンク300を介して行われる。通信リンク300は、クライアント120およびサーバ140の双方に連結されるインターネットサービスプロバイダ(ISP)を例示的に含む。

【0079】ある時点では、ユーザは、アイテム購入を希望する旨を示す。次いで、サーバ140は、通信リンク300または他の経路を介して、データストリーム302を送付する。データストリーム302は、取引に立ち会う中立的立会人100に関する情報を含む。データストリームの目的の1つは、クライアントに対して中立的立会人を識別し、それにより、クライアントが中立的立会人との接続を確立することにある。例示的に、データストリーム302内の情報は、Uniform Resource Locator(URL)、またはクライアント120を中立的立会人にアクセスさせ得る他の位置決め手段を含み、且つ取引を識別するための識別子(例えば、コードまたは文字数字配列)を含む。

【0080】サーバ140は、通信リンク304を介して、中立的立会人100との安全な接続を確立し、且つ中立的立会人に取引識別子を通知する。それにより、中立的立会人は取引を行っている適切な当事者を見つけ得る。同様に、クライアント120は、通信リンク306を介して、中立的立会人100との安全な接続を確立し、且つ、また、中立的立会人に取引識別子を受け渡す。発明の本実施態様において、リンク304および306はSSL保安プロトコルを用いる。SSLプロトコルの実行は、リンク304およびリンク306を通じての信の改変を防ぐ(おそらく、中立的立会人100による改変以外は)。本実施態様では、中立的立会人100は各当事者を認証し、各当事者は中立的立会人を認証する。例示的には、中立的立会人は当事者双方とデジタル証明書を交換する。または、SSL認証手段が用いられるか、または、適用可能な場合は、固定IPアドレスが交換され、調査される。

【0081】当事者と中立的立会人との間に信用通信経路が存在するので、当事者は、安全性維持のために、互いの間の取引の全部分または選択された部分を中立的立会人に受け渡し得る。しかし、示される動作方法では、クライアント120とサーバ140との間の交渉および通信用の主要経路はリンク300である。したがって、各当事者から中立的立会人に特に送付される情報のみが保存される。どの情報が中立的立会人に送付されるべきかを決定する方法は、上述の通りである。しかし、1つの実施態様では、サーバ140がクライアント120に送付する情報(例えば、ウェブページ)は、中立的立会人にも送付される。加えて、クライアント120はサーバ140から受け取る情報を中立的立会人に転送するか、または、サーバ140から受け取られた情報に関するメッセージダイジェスト(後述)を送付する。したがって、中立的立会人は、サーバ140によって提供される取引詳細を照合し、その正確さを検証し得る。

【0082】中立的立会人100はクライアント120およびサーバ140から離れて示されるが、本発明の別の実施態様では、中立的立会人はクライアント120およびサーバ140のいずれかと、または双方と共に配置される(例えば、同一のコンピュータシステムまたはネットワーク上)。

【0083】図4は上述のプロセスをより詳細に示したフローチャートである。段階400は開始段階である。本発明の例示的な実施態様では、開始段階400以前に、またはそれと同時に、当事者は、彼らの取引をモニタするため中立的立会人を選択するかまたはそれに合意する。本発明の別の実施態様では、中立的立会人100の選択は取引開始後に実行される。段階402では、クライアント120に接続されたユーザは、通信リンク300を介してサーバ140上の情報にアクセスし情報を見るためにインターネットを用いる。したがって、クライアント120は、Netscape NavigatorまたはMicrosoft Internet Explorerなどのブラウザ、或いはサーバ140にアクセスするよう設計された他のインターネットエクスプローラーを例示的に含む。サーバ140は、様々な物品および/またはサービスを販売目的に提供する小売商によって例示的に用いられる。したがって、段階402において、ユーザは小売商の提供物を再検討する。

【0084】段階404において、ユーザはアイテムの購入を決定し、その旨信号を発する。例示的には、ユーザは、クライアント120および/またはサーバ140上で実行されるソフトウェアを操作することによって、「買」いオプションを選択する。購入を行うという決定は、当事者が安全且つ信用通信モードに入る必要があることを意味する。この信用モードでは、中立的立会人100は取引の1つ以上の詳細を記録または保存し、それにより、係争の際にはそれらの詳細が再生され得る。

50 これは、当事者のいずれかが後に取引を拒絶することを

防ぐ。

【0085】ユーザの購入動作に応答して、段階406では、サーバ140は通信リンク34を介して中立的立会人100に接続する。それは、中立的立会人のURL、または他の位置決め手段を用いて行われる。本実施態様では、サーバ側の当事者（すなわち、小売商）は中立的立会人を選択する。別の実施態様では、中立的立会人はクライアント側の当事者によって選択されるか、または当事者間における合意によって決定される（例えば、受け入れ可能な立会人を含むリストを交換し、双方のリストに共通する1人に合意することにより）。中立的立会人は、取引の詳細を正確に記録することを求められるので、通信リンク304はSSLプロトコルの使用によって保護される。したがって、信頼経路はサーバ140と中立的立会人100との間に確立される。

【0086】サーバ140および中立的立会人100の身元を確実にするために、サーバ140および中立的立会人100は、段階408において互いに自らを認証する。例示的には、SSL認証を用いてそれを行う。本発明の別の実施態様では、サーバおよび中立的立会人は、保証権限者により発行されたデジタル証明書を交換することにより、互いに認証する。他の別の実施態様では、サーバ140および中立的立会人100は單にIPアドレスを検証するか（双方が固定IPアドレスを有する場合）、或いは、Monexカードまたは他の身分証明カードを用いる。更に別の他の実施態様では、サーバ140は中立的立会人100を認証するが、中立的立会人はサーバ140を認証する必要はない。当事者は、段階406および408の主要な目的がサーバ140と中立的立会人100との間に安全な経路を確立し、且つ、第3者がサーバ140または中立的立会人100のいずれかをかたることを防ぐものであることを認識する。通信リンクが確立され、且つ通信者が誰と通信しているのかをかなり確信している限り、その目的を達成するために様々な方法が適切である。

【0087】段階410において、サーバ140は中立的立会人に取引識別子を送付し、取引識別子は、接続された際に、クライアントを識別するために用いられる。発明の本実施態様では、識別子はサーバ140によって発生されるか、または選択される。識別子はこの取引にとって独自のものであり、少なくとも、特定の時間内に存在するか、または特定のクライアントと存在する。例示的には、取引識別子は文字数字コードまたは数字の配列を含む。

【0088】段階412では、サーバ140はクライアント120にデータストリーム302を発行する。データストリーム302の主要目的は、クライアントに対して、取引に立ち会い、モニタする中立的立会人を識別することである。データストリーム302内には、中立的立会人100を識別するURLが備わる。URLは、中立的立

会人がどこで（例えば、インターネット上）で発見され得るかを識別する。または、中立的立会人はいくつかの他の方法によって識別され得る（例えば、固定IPアドレスまたは他の独自の位置決め手段により）。データストリーム302は、また、取引識別子を含む。取引識別子が必要となるのは、中立的立会人100がクライアント120およびサーバ140への別々の接続に関与するためである。したがって、中立的立会人100は、立ち会う取引のそれぞれに関与する当事者を正確に識別し、適合させ得る必要がある。クライアント120およびサーバ140が、中立的立会人100に個別に接続する場合、クライアント120およびサーバ140はそれぞれ同一の取引識別子を提供する。取引識別子は、サーバ140によって送付されたURLに取り付けられるフラグを示例的に含む。あるいは、識別子は個別の送信で送付される。

【0089】段階414において、クライアント120は、サーバ140によって提供される位置決め手段（例えば、URL）を介して中立的立会人100に接続する。

クライアント120は、通信リンク306をわたって中立的立会人100に接続する。通信リンク306は、信頼リンクを提供するために、リンク304（例えば、SSL）と同様の方法によって保護される。次いで、クライアント120および中立的立会人100は、段階416において、互いに認証する。それは、段階410において用いられたものと同一の、または異なる機構を用いて行われる。次いで、段階418において、クライアント120は、サーバ140から受け取った取引識別子を送信する。識別子を受け取ると、中立的立会人100は、取引に関与する他の当事者を決定し、それにより、サーバ140を発見する。例示的に、サーバ140は、中立的立会人に対して、取引に関与する当事者の数を通知し、それにより、中立的立会人は、全当事者が接続され、または他の方法で代表されていることを確実にし得る。

【0090】クライアント120および中立的立会人100は、示される実施態様のように、安全且つ信頼性のある方法で接続されるが、別の実施態様では、高レベルの信頼性は必要とされない。例えは、取引中にクライアントが支払いを行ひ（例えば、クレジットカード、Digicash、Cybercashなどを介して）中立的立会人がその支払いについて通知される電子取引においては、取引におけるユーザ側の責任部分の実行に関する係争の危険性はほとんど、または全くない。小売商側の実行のみが係争の対象になるので、したがって小売商は、取引の基本的な詳細（例えば、金額、質、アイテムの説明、配達条件、保証）の記録を中立的立会人に提供する動機を有する。もちろん、クライアントも、安全確保のために、取引の詳細を中立的立会人に提出し得るが、係争の際には、責任部分に関する実行についての説明は小売商側に

課せられる。小売商の責任は、小売商によってサーバに提供された詳細およびその詳細の信頼性によって、部分的または完全に軽減される。

【0091】再度図4を参照して、中立的立会人100と、クライアント120およびサーバ140のそれとの間に信用性のある接続が存在すると、段階420において、当事者は、取引の詳細を中立的立会人に提出する。例えば、当事者のいずれか、または双方が、当事者間で交換されたウェブページを提出し得る。取引を含む通信は、当事者が中立的立会人100と信用性のある接続を確立する前、確立している間、および/または確立した後に、発生し得る。

【0092】本発明の例示的な実施態様の1つでは、公知の取引プロトコルが、クライアント120とサーバ140との間の取引について効力を有する（例えば、オーバンターディングプロトコル）。そのプロトコルの1部として、クライアント120およびサーバ140のいずれか、またはその双方は、取引の中心的部分を認識し、且つ自動的にその部分を中立的立会人100に転送する。そのようなプロトコルが、図1に示される本発明の実施態様において用いられる場合、中立的立会人100は効力を有するプロトコルを認識し、自動的に関係のある情報を記録する（クライアントとサーバとの間で流される情報またはデータの全てを記録または保存する代わりに）。

【0093】別の実施態様の1つでは、取引の全当事者が、取引または取引の詳細に関する自らの理解を証拠づける「契約書」または他の書類を中立的立会人に提出する。契約書は、送信の間における変更を防ぐために、暗号によって署名されていることが好ましい。全当事者が実質的に同一の契約書を受け取ることが、本実施態様における合意を形成する。

【0094】本発明の別の実施態様では、中立的立会人100に全ウェブページ、電子書類、または他の情報を受け渡す代わりに、当事者のいずれか、または双方は、立会人にメッセージダイジェストを送付するのみである。例示的には、そのようなメッセージダイジェストは取引詳細の要旨のみを含む。そのような実施態様においては、当事者の一方または双方が元の詳細を維持する。取引に関する係争の際には、元の詳細から新たなメッセージダイジェストが作成され、中立的立会人に提供されたメッセージダイジェストと比較される。

【0095】または、メッセージダイジェストは、取引（または、その中心的部分）を含む通信に対して行われた、ハッシュまたは検査合計動作の結果を含む。したがって、当事者には、中立的立会人100に提出され、そこで維持される情報の詳細についての量および程度は広範囲なものであり得ることが理解される。中立的立会人は、当事者の間で取り交わされた全情報（図1に示されるような実施態様において）、その情報について行われ

たハッシュ機能または検査合計動作の結果のみ、または両者の間の若干量の結果を受け取り得、且つ記録し得る。

【0096】段階422において、当事者によって提出された情報は指標化され、保存される。例示的には、当事者から受け取られたもの全ては受取時間が刻印され、時間、日付、サーバ、クライアント、および取引識別子といった識別特性によって指標化される。段階424では、中立的立会人100は、取引に関与している当事者の一方、または法的仲介者に対して、記録された取引詳細を提供する。典型的には、詳細は、取引に関する条件または当事者の責任範囲についての係争を解決するため用いられる。段階426は終了段階である。

【0097】中立的立会人によって記録された取引への当事者間における、後の係争に際して、当事者のいずれか、または双方は、中立的立会人に対して取引またはその中心的部分を再生するよう要求し得る。例えば、ユーザが小売商から潜水用足ひれ1対を受け取ったが、実際は山岳用ブーツ1対を注文していたとしてクレームした場合、ユーザおよび/または小売商は中立的立会人に対して、何が注文されていたのかを証明するよう要求する。中立的立会人の信用性、および情報が中立的立会人に提供される方法の安全性から、中立的立会人によって提供される証拠は、取引が、中立的立会人によって報告された通りに行われたという推定を形成する。要求された情報を取り出すためには、中立的立会人は、単に、取引に関する詳細のいくらか（例えば、日付、取引識別子、サーバおよび/またはクライアントの鼻印）を要求する。

【0098】上述のように、中立的立会人は、当事者の一方から提供されたハッシュ値または検査合計のみを記録し得る。ハッシュ値または検査合計を提供した当事者は、そのハッシュ値または検査合計動作を行なった取引の完全な詳細を記録する責任を有する。当事者の一方が完全な詳細を保存し、それを中立的立会人に提供もする別の実施態様では、中立的立会人は依然、完全な詳細でなく、検査合計またはハッシュ値（中立的立会人が算出した）のみを記憶する。詳細は当事者によって維持されているので、中立的立会人はこの方法で記憶空間を保ち得る。

【0099】例えば、1つの実施態様では、サーバは中立的立会人に対して、取引を含む通信に関するハッシュおよび/または検査合計値を含むメッセージダイジェストを提供するのである。取引に関して後に係争が生じる場合、サーバは取引の詳細を生成し、それを中立的立会人、同様にはクライアントおよび/またはその事件について調査している法的関係当局に提供する。次いで、中立的立会人は、最初にサーバによって行われたものと同一の機能を用いて詳細についてのハッシュ値を算出し、元の値と比較する。それらの値が同一である限り

は、中立的立会人は、サーバによって提供された詳細は正確であることを保証し得る。または、サーバは第2のハッシュ値を生成し、それを、次いで比較を行う中立的立会人に提供する。

【0100】上記説明では、図4に示されるように、本発明の実施態様にしたがって電子取引を行うために、通信の「信用モード」に入る方法の1つが提示された。別の実施態様では、当事者は、「ブラウズモード」から「信用モード」へ異なる方法によって移行する。この別の実施態様において、依然、ユーザが購入を開始する

が、その取引を行うにあたり、中立的立会人および/またはサーバサイトの選択肢を提供される。例示的には、ユーザはURLのリストから選択する。各URLは中立的立会人とその安全な接続に対応し、立会人のネットワークアドレスを含む。URLは、更に、取引における小売商を表すサーバサイトのアドレスを含む。フラグまたはクリップトを含む。一旦ユーザが、選択されたURLを介して、中立的立会人に接続すると、中立的立会人は特定されたサーバサイトに安全に接続する。次いで、サーバは、認証データ、サーバの身元、取引用の取引識別子、取引を維持する際の別のサーバページまたはサイトなどの情報を中立的立会人に送付する。次いで、サーバおよびクライアントは上述のように取引を行い、取引の詳細を安全確保のために中立的立会人に受け渡す。

【0101】図5は、取引に2人以上の当事者（例えは、クライアントに接続されるユーザおよびサーバに接続される小売商）が関与する、本発明の1つの実施態様を示す。第1の当事者500および第2の当事者502は、例示的に、それぞれクライアントおよびサーバである。他の様々な当事者もまた、参加し得る。第Nの当事者は、符号504によって表される。第Nの当事者504は別のサーバを表し得、おそらくそのサーバは、ユーザが、電子取引を行うアカウントを維持しているサーバである。

【0102】別の実施態様では、第Nの当事者504は「対価取得手段」である。対価取得手段は、しばしば、電子取引において用いられる。そのような観点では、ユーザが購入を希望する場合、ユーザは購入したアイテムの売価を対価取得手段（例えは、電子銀行）に支払う。支払いは、おそらく、クレジットカード、Digicash、または他の手段によって行われる。次いで、対価取得手段は小売商に対して、ユーザがアイテムについての支払いを行ったことを保証し、次いで、小売商はユーザにアイテムを配達する。

【0103】図5に示される1つの実施態様において、中立的立会人100は当事者を接続する通信経路内に存在し得る（通信リンク510、512、および514によって表される）。または、当事者は、通信リンク520、522、および524を介してそれらの間を通信し、特定の取引詳細または通信を、通信リンク510、

512、および514を介して中立的立会人100に提出するものである。

【0104】本発明の実施態様についての以上の説明は、例示および説明の目的にのみ提示された。それらは、本発明が開示された形態で説明し尽くすものではなく、且つ規定することを意図するものではない。当事者には、多くの改変および変更が明らかとなる。したがって、以上の開示は発明を規定することを意図するものではない。発明の範囲は、添付の請求の範囲によって規定される。

【0105】電子取引の全詳細または選択された詳細に立ち会い、且つ記録する、中立的立会人が提供される。取引は、インターネットまたは他の分散型通信チャネルを介して通信する。多数の当事者を伴い得る。1人の当事者が取引を開始した場合、当事者は、借用通信リンクを介して中立的立会人に接続する。次いで、1人以上の当事者が、取引に関する全詳細または選択された詳細を受け渡す。中立的立会人に提出される詳細は、その取引が行われるプロトコルにしたがって識別される。中立的立会人は、後に取引に関する係争の解決に用いたために、その詳細を確実に記憶する。中立的立会人は、全通信（例えは、ウェブページ）、通信の選択された部分、またはメッセージダイジェストを記憶し得る。または、中立的立会人は、当事者間の通信経路内に位置づけられ、したがって、記録される情報および詳細を自動的に取り出し得る。

【0106】

【発明の効果】本発明によると、電子商取引の詳細が中立的立会人により保存される方法が提供される。中立的立会人は、取引に関与する2以上の当事者と特定のプロトコルを用いて借用通信リンクを確立する。この取引では、取引およびその取引に関与するを識別するため、取引の当事者は中立的立会人に對して取引識別子を提供する。それにより、中立的立会人は取引の全当事者を識別することが出来る。従って、中立的立会人は特定のプロトコルに従って、関係のある取引詳細を自動的に取り出し、保存することができる。

【図面の簡単な説明】

【図1】本発明の1つの実施態様による、2人の当事者の間の電子取引のブロック図であり、その電子取引では中立的立会人が取引の拒絶を防ぐ。

【図2】本発明の別の実施態様による、2人の当事者の間の電子取引のブロック図であり、その電子取引では、中立的立会人が取引の拒絶を防ぐ。

【図3】本発明の1つの実施態様による、中立的立会人が電子取引に立ち会うために呼び出される、ブロック図である。

【図4】図3に示される、本発明の実施態様を実行する際に伴う動作のいくつかを示す、フローチャートである。

25

26

【図5】本発明の1つの実施態様による、中立的立会人によって監視される当事者が2人以上間与する電子取引のブロック図である。

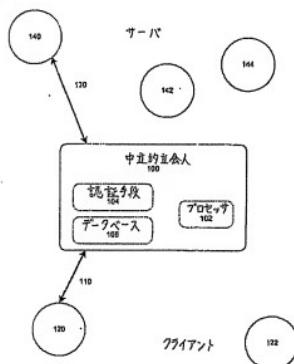
【符号の説明】

- 100 中立的立会人
- 102 プロセッサ
- 104 認証手段
- 106 データベース

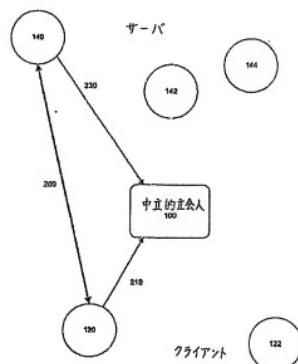
*

- * 110、130、510、512、514、520、522、524 通信リンク
- 120 サーバ
- 140 クライアント
- 500 第1の当事者
- 502 第2の当事者
- 504 第Nの当事者

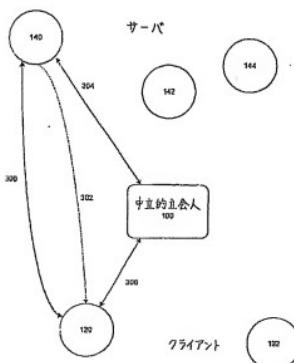
【図1】



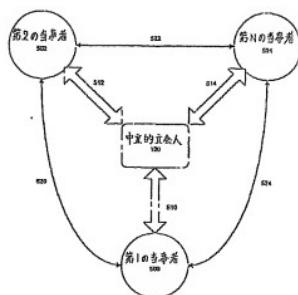
【図2】



【図3】



【図5】



[図4]

